Рекомендации

Оценка риска контрагента в отношении кибербезопасности

Руководство по началу работы

Содержание

Краткое резюме	4
Контекст	5
Разработка модели управления рисками в отношении кибербезопасности	5
Разработка концепции управления рисками в отношении кибербезопасности	7
Данные об уровне риска контрагента	7
Процесс оценки рисков	8
Принятие контрмер с целью снижения рисков в отношении кибербезопасности	9
Приложение A: Интеграция данных по аттестации, полученных от контрагентов SWIFT	10
Соображения в отношении модели управления	11
Соображения в отношении концепции управления рисками	13
Дополнительные меры по снижению рисков	14
Приложение B: Глоссарий	16
Приложение C: Голос клиента	17

Оговорки и ограничительные условия

Настоящий документ содержит общие и необязательные рекомендации для пользователей системы SWIFT о том, как использовать и интерпретировать данные по кибербезопасности, полученные от контрагентов в рамках системы финансовых услуг. В нем содержатся предложения относительно рекомендуемого подхода к управлению, а также процессов обмена и интеграции данных о рисках в отношении кибербезопасности в существующую концепцию управления рисками учреждения.

Он не затрагивает специфические для пользователя проблемы или требования.

Информация, приведенная в настоящем документе, не является исчерпывающей и не отменяет необходимости руководствоваться здравым смыслом или следовать передовой практике.

Пользователи несут полную и исключительную ответственность за любые действия или решения, принятые в результате ознакомления с этими руководящими принципами или рекомендациями, а также за интерпретацию данных, изложенных в настоящем документе. SWIFT не несет никакой ответственности за содержание настоящего документа, а также за любые предпринятые действия и решения, принятые на основе или в связи с содержанием настоящего документа, а также за их последствия. Ничто в настоящем документе не должно быть интерпретировано или истолковано как обязательство, заверения или гарантии со стороны компании SWIFT.

Компания SWIFT предоставляет настоящий документ исключительно в ознакомительных целях. Информация, содержащаяся в этом документе может со временем претерпевать изменения. Пользователи должны всегда обращаться к последней доступной версии.

Голос клиента

С какими основными проблемами вы сталкиваетесь при управлении киберрисками применительно к вашим контрагентам?

«Основной проблемой, с которой мы сталкиваемся, является получение доступа к элементам киберконтроля наших контрагентов. Недостаток знаний об уровне контроля у контрагентов еще больше усложняет управление киберрисками. Вы сильны настолько, насколько сильно ваше самое слабое звено. Вот почему так важно проводить комплексные проверки в отношении кибербезопасности контрагентов.

Ключевыми задачами являются следующие:

- Разработка согласованного стандарта, используемого всеми контрагентами, который можно применять для проведения сопоставительного анализа
- Получение от контрагентов информации об их элементах контроля безопасности или их отсутствии
- Проверка точности информации, предоставленной контрагентами
- Сбор и обработка данных таким образом, чтобы предоставить организации ценную информацию о рисках в доступной форме, на основе чего они смогут принимать соответствующие бизнес-решения
- Последующее наблюдение за проблемными областями, чтобы убедиться, что недостатки устранены и вопросы закрыты, а также согласовать применение компенсационных элементов контроля в промежуточный период».

Краткое резюме

Угрозы кибербезопасности остаются ключевыми в секторе финансовых услуг. В настоящем руководстве описывается, как организации в банковской и платежной системах могут подходить к оценке риска в отношении кибербезопасности, создаваемого контрагентами, с которыми они ежедневно взаимодействуют.

Настоящее руководство охватывает четыре области, на которые должны обратить внимание все учреждения: разработка модели управления; разработка концепции управления рисками в отношении кибербезопасности; принятие мер с целью снижения рисков в отношении кибербезопасности и интеграция данных по аттестации в отношении кибербезопасности, полученных от контрагентов.

Рисками в отношении кибербезопасности, в том числе связанными с контрагентами, следует управлять наряду с другими видами рисков — операционными, финансовыми и нормативными. Многие учреждения работают над интеграцией оценки киберрисков в существующие процессы оценки рисков контрагента.

Для обеспечения того, чтобы соответствующие лица с соответствующими полномочиями могли принимать обоснованные решения, а процессы были надежными и повторяемыми, необходимо разработать средства надзора за этим процессом — **управление**. Имея надежную структуру управления, учреждения могут приблизиться к внедрению **концепции управления рисками в отношении кибербезопасности**. Это предполагает оценку рисков контрагентов посредством:

- сбора необходимых данных с целью обоснования решений, связанных с риском;
- обработки этих данных и их преобразования во взвешенную оценку рисков, обычно в виде баллов или красно-жёлто-зелёного индикатора;
- принятия соответствующих контрмер для смягчения или «урегулирования» рисков.

Учреждения могут иметь разные приемлемые уровни риска, но к примерам контрмер по снижению риска в отношении кибербезопасности относится следующее:

- внедрение дополнительных уровней контроля за транзакциями контрагента;
- ограничение типа транзакций, проводимых контрагентом;
- требование, чтобы контрагент внедрил дополнительные элементы контроля или меры по выявлению мошенничества;
- требование, чтобы контрагент подтвердил свою информацию доказательствами путем проведения независимой оценки;
- переоценка соглашений и контрактов с контрагентом.

Учреждениям следует рассмотреть возможность включения в эту модель управления рисками данных о готовности своих контрагентов реагировать на киберугрозы.

Концепция обеспечения безопасности пользователей SWIFT (CSCF), представленная системой SWIFT в рамках ее Программы обеспечения безопасности пользователей SWIFT (CSP), неоценима в этом отношении. Концепция обеспечения безопасности пользователей SWIFT содержит набор обязательных и рекомендуемых для пользователей системы SWIFT мер обеспечения безопасности, устанавливающих исходный уровень безопасности для всего финансового сообщества. Ее должны внедрить в свою местную инфраструктуру системы SWIFT все пользователи, которые должны самостоятельно подтверждать свое соответствие обязательным требованиям по обеспечению безопасности.

После публикации самоаттестации пользователи могут предоставить к ней доступ любому из своих контрагентов, свидетельствуя тем самым о своем соответствии требованиям индивидуального контроля, — а контрагенты аналогичным образом могут потребовать предоставить доступ к аттестации друг от друга. Пользователи могут просматривать и экспортировать данные как по каждому отдельному контрагенту, так и по группам, чтобы лучше «**потреблять**» данные и интегрировать их в свои системы принятия решений, связанных с риском.

Концепция обеспечения безопасности пользователей SWIFT (CSCF) помогает повысить прозрачность и стандартизацию финансового сектора, чтобы помочь организациям интегрировать вопросы кибербезопасности в процесс принятия решений. Данные по аттестации богаты информацией и являются уникальным источником данных о рисках в отношении кибербезопасности для пользователей системы SWIFT.

Контекст

Главными современными глобальными угрозами по-прежнему остаются киберпреступность и мошенничество. Техническое мастерство злоумышленников растет, массовые утечки данных являются обычным явлением, из-за целевых кибератак типа «Развитая постоянная угроза» (Advance Persistent Threat, APT) практически каждый человек может стать жертвой киберпреступников, а вездесущие «умные» устройства «Интернета вещей» можно использовать как оружие при распределенной атаке на отказ в обслуживании (distributed denial-of-service attack, DDoS).

В секторе финансовых услуг эти злоумышленники представляют угрозу из-за организуемых ими изощренных кибератак, основной целью которых является **кража активов** жертвы.

Но, конечно, организации банковской и платежной систем работают не изолированно друг от друга — они ежедневно взаимодействуют с многочисленными контрагентами и осуществляют совместные транзакции. Эти риски вполне реальны, так как кибератаки небольшого числа опытных и хорошо финансируемых злоумышленников на клиентов SWIFT продолжаются. **Как организации определить и снизить возможный риск того, что она может осуществлять транзакции с ничего не подозревающей жертвой кибератаки?** Если риск в отношении кибербезопасности не будет устранен, а деньги будут потеряны, финансовые риски могут быть значительными.

В настоящем руководстве рассматривается, какой подход может применять организация к оценке риска в отношении кибербезопасности, создаваемого контрагентами. Оно охватывает четыре ключевые области:

- Разработка модели управления рисками в отношении кибербезопасности
- Разработка концепции управления рисками в отношении кибербезопасности
- Принятие контрмер с целью снижения рисков в отношении кибербезопасности
- Интеграция данных по аттестации кибербезопасности, полученных от контрагентов SWIFT

В оставшейся части настоящего документа обсуждаются эти четыре темы.

Голос клиента

Помогли ли данные по аттестации в отношении кибербезопасности решить одну или несколько из этих проблем, и если да, то как?

«Процесс аттестации безопасности клиентов системы SWIFT дополнил нашу общую программу управления контрагентами, призванную решить эти проблемы. Благодаря получению данных по аттестации у нас теперь есть возможность определить уровень контроля, применяемого контрагентом. Зная тип и уровень контроля, применяемого каждым контрагентом, мы можем более эффективно управлять киберрисками.

Программа обеспечения безопасности пользователей SWIFT(CSP) предоставила нам систематизированный набор ответных действий, применяемый всеми контрагентами, который можно использовать для проведения сопоставительного анализа. Для нас это как квалификационные испытания для приемных комиссий университета. Инструмент аттестации очень прост в использовании, когда вам нужно запросить доступ у контрагентов или предоставить им его. Программа обеспечения безопасности пользователей SWIFT (CSP) помогает нам быть уверенными в ответах контрагентов, предоставляя им средства для проверки своих ответов посредством проведения внутреннего и/или внешнего аудита. Мы разработали количественную модель для сбора данных из инструмента аттестации и последующего создания отчетов и диаграмм».

Разработка модели управления рисками в отношении кибербезопасности

Рисками в отношении кибербезопасности, включая риски контрагентов, необходимо управлять наряду с другими видами рисков — операционными, финансовыми и нормативными.

Для обеспечения того, чтобы соответствующие лица с соответствующими полномочиями могли принимать обоснованные решения, а процессы были надежными и повторяемыми, необходимо разработать средства надзора за этим процессом — управление.

Структура комитета старших должностных лиц

Управление рисками в отношении кибербезопасности следует рассматривать как целостную функцию. Это означает, что за этим процессом должны централизованно наблюдать те, кто несут ответственность за бизнес в целом, а не ограниченные в полномочиях изолированные функциональные подразделения обработки документов в отделе ИТ или оперативном отделе. На практике управление рисками контрагента должно быть частью (или подразделением) **структуры комитета старших должностных лиц, например, Комитета по управлению рисками,** со своей сферой полномочий и необходимыми ресурсами.

В рамках этой междисциплинарной структуры управления следует также рассмотреть вопрос о распределении обязанностей между «3 линиями защиты». На практике это означает, что ежедневные решения в отношении операционного риска должны приниматься на первой линии защиты (например, отделом поддержки бизнеса, оперативным отделом, отделом ИТ/отделом по обеспечению кибербезопасности), поскольку они отвечают за реализацию мер внутреннего контроля и операционных процедур. Исключения и передачу информации на более высокий уровень руководства следует рассматривать на второй линии защиты (например, отдел нормативно-правового соответствия, отдел управления рисками), поскольку она обладает определенной степенью операционной независимости. Достоверность информации должна контролироваться третьей линией защиты (например, отделом внутреннего аудита), так как она является независимой.

Заинтересованные стороны от бизнеса

Функции управления должны осуществляться лицами с уровнем полномочий, адекватным для принятия эффективных решений в рамках соответствующих внутренних групп заинтересованных сторон.

Возможно, многие повседневные решения в отношении операционного риска для управления контрагентами должны приниматься **представителями бизнеса**, а не исключительно техническими специалистами или специалистами по обеспечению кибербезопасности. Тем не менее, общее управление должно быть целостным и включать представителей следующих областей:

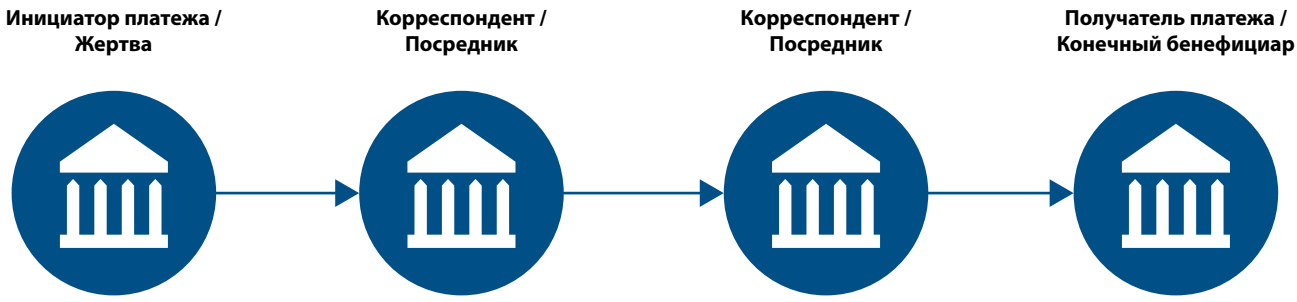
- **Управление отношениями с деловыми кругами** и контрагентами - с целью оценки подверженности рынка и контрагента рискам и поддержания взаимоотношений с контрагентом
- **Платежные операции** - с целью осуществления оперативного контроля, корректировки лимитов и вмешательства в обычные операции по обработке платежей
- **Технические,** например, отдел ИТ/информационной безопасности/обеспечения кибербезопасности - с целью реализации дополнительных технических элементов контроля или конкретных мер по выявлению мошенничества
- **Риски, нормативно-правовое соответствие и аудит** - с целью управления исключениями и осуществления независимого подтверждения достоверности.

В связи с конфиденциальностью данных и потенциальными последствиями нарушений в области безопасности надзор за этим процессом должен осуществлять руководитель высшего звена, он должен также помогать управлять процессом оценки рисков и рассмотрения вышестоящими инстанциями и контролировать принимаемые контрмеры.

Четко определенная сфера полномочий

У комитета старших должностных лиц, осуществляющего надзор за рисками контрагента, должна быть четко определенная сфера полномочий или Рабочее задание, описывающее долгосрочную стратегию, а также текущую модель работы, включая распределение ролей и обязанностей.
Эта сфера полномочий также включает проведение регулярных брифингов для совета директоров и высшего руководства по вопросам оценки ландшафта рисков контрагента, конкретных инцидентов, а также улучшений и тенденций.

Концепция оценки риска контрагента в отношении кибербезопасности



Настоящее руководство предназначено для:

- **Малых и средних предприятий**, получающих инструкции от инициатора платежа. У этих субъектов малого и среднего бизнеса ограниченное число контрагентов по сравнению с более крупными учреждениями, у которых множество партнерских отношений и сложная внутренняя структура.
- **Банков-корреспондентов** (независимо от размера), которые выступают в качестве посредников в транзакции между инициатором платежа и конечным бенефициаром.

Голос клиента

Можете ли вы конкретно описать, как вы используете данные аттестации кибербезопасности, помимо представления вашей самоаттестации посредством инструмента? Как конкретно вы используете их в контексте управления рисками в отношении безопасности ваших контрагентов?

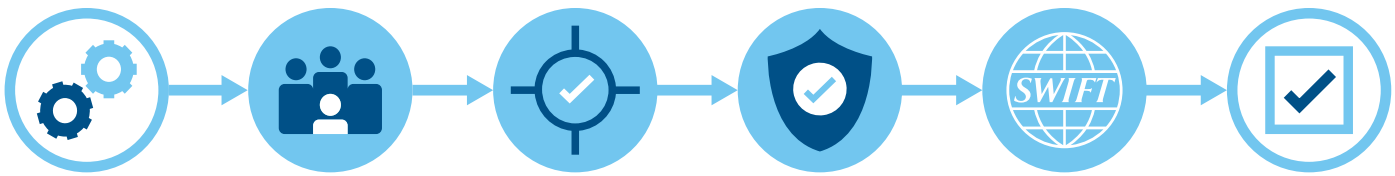
«Инструмент аттестации предоставляет последовательные ответы, поэтому мы можем оценить каждую аттестацию и выставить баллы на основе этих ответов. Это позволило нам применять повторяемые количественные и качественные измерения к каждой аттестации. Ранее мы полагались исключительно на вопросники, которые во многих случаях давали противоречивые ответы».

Разработка концепции управления рисками в отношении кибербезопасности

Имея надежную структуру управления, учреждения, как правило, подходят к обеспечению кибербезопасности с точки зрения оценки риска. Это означает, что они оценивают уровень риска, инвестируют средства в те области, где они наиболее необходимы, и принимают риски ниже установленного порога или приемлемого уровня риска. Этот процесс или концепция управления рисками в отношении кибербезопасности состоит из нескольких этапов:

1. **Сбор необходимых данных о риске контрагента.**
2. **Оценка уровня риска посредством обработки данных. Обычно это делается путем присвоения общего балла и его сопоставления с приемлемым уровнем риска компании.**
3. **Принятие соответствующих мер для управления или «устранения» рисков, исходя из оценки риска.**

Концепция оценки риска контрагента в отношении кибербезопасности



Разработка **модели управления рисками** в отношении кибербезопасности

Разработка **концепции управления рисками** в отношении кибербезопасности

Принятие **контрмер** с целью снижения рисков в отношении кибербезопасности

Интеграция данных по **аттестации в отношении кибербезопасности**, полученных от контрагентов SWIFT

Данные об уровне риска контрагента

Учреждения собирают и обрабатывают различные данные, чтобы определить профиль риска контрагентов с точки зрения кибербезопасности.

Данные о рисках можно подразделить на три категории: данные, относящиеся к внешней среде, в которой осуществляет свою деятельность контрагент; данные, описывающие деловые отношения с контрагентом; данные, относящиеся к транзакции.

1. Риски, связанные с внешней средой, в которой осуществляет свою деятельность контрагент:

- **Страна/регион деятельности** — может служить мерой уровня кибербезопасности, регулирования и преступности/мошенничества в юрисдикции, в которой осуществляет свою деятельность контрагент. Этот тип риска можно оценить, используя общедоступные источники, например, отчет о рисках в отношении отмывания денег Базельского комитета по банковскому надзору;
- **Тип отрасли** — может коррелировать с вероятностью кибератаки, так как некоторые сектора экономики страдают от кибератак и утечки данных чаще, чем другие;
- **Степень регулирующего** надзора за контрагентом и степень, в которой местный надзорный орган обязует внедрять положения или политику в отношении кибербезопасности.

2. Риски, связанные с деловыми отношениями с контрагентом

- **Глубина/длительность отношений с контрагентом** — новые отношения могут характеризоваться более высоким уровнем риска, чем давние, глубокие и проверенные временем отношения;
- **Размер/структура собственности контрагента** — может коррелировать с наличием достаточного бюджета, квалифицированных кадров и инструментов, необходимых для борьбы с киберугрозами, особенно если учреждения являются частью более крупной группы, например, Глобальные системно значимые банки (Global Systemically Important Banks, GSIB);
- **Информация об имевших место происшествиях** в сфере кибербезопасности и безопасности и другие доступные данные из новостей, информация или материалы по результатам комплексной проверки;
- **Существующие оценки рисков контрагента,** например, операционных, финансовых или нормативных рисков.

3. Риски, связанные с транзакциями

- **Типы транзакций** — ограничение по типу транзакций, осуществляемых с контрагентом, поскольку некоторые типы транзакций по своей природе более уязвимы, чем другие, например, платежи по сравнению с выписками по счету;
- **Сумма транзакции** — служит отражением подверженности кредитному риску;
- **Частота транзакций** — чем больше объем транзакций за определенный период, тем больше потенциальная поверхность атаки.

После сбора данных о контрагенте может быть применен процесс оценки рисков.

Процесс оценки рисков

После сбора данных о контрагентах учреждения обрабатывают их и преобразуют в оценку рисков. Методология оценки рисков в разных учреждениях может отличаться, но обычно применяется один из трех подходов:

- **Экспертный** — оценка рисков основывается на экспертной и качественной оценке рисков специалистами;
- **Основанный на правилах** — оценка производится с помощью дерева решений с использованием простых правил относительно того, какой балл присваивается контрагенту по каждому из факторов риска;
- **Основанный на модели** — оценка выводится аналитически на основе того, какой балл присваивается контрагенту по каждому взвешенному фактору риска.

Независимо от принятого подхода контрагенту обычно присваивается общий балл, который отображается в виде красного, желтого или зеленого индикатора уровня риска.

Контрмеры по снижению рисков зависят от сравнения этого показателя с внутренним приемлемым уровнем риска. Например, контрагенты с низким (или зеленым) уровнем риска могут быть классифицированы как не требующие дополнительной проверки, а в отношении контрагентов с высоким (или красным) уровнем могут быть приняты контрмеры по снижению риска.

Принятие контрмер с целью снижения рисков в отношении кибербезопасности

Концепция управления рисками позволяет учреждению оценить и классифицировать степень риска в сфере безопасности, связанного с контрагентом. Затем учреждение может либо принять решение о принятии рисков, либо рассмотреть меры по снижению рисков.

Контрмеры с целью снижения рисков в отношении кибербезопасности могут включать следующее:

1. Контрмеры, связанные с деловыми отношениями с контрагентом

- Заблаговременное **сотрудничество с высшим руководством** с целью укрепления отношений и обеспечения общей уверенности в достоверности данных;
- Запросы к контрагенту об **обосновании предоставленной информации** посредством проведения внутренней или сторонней/внешней независимой оценки или предоставления технической спецификации документации или результатов анализа данных;
- Запросы к контрагенту о применении **дополнительных элементов контроля** или меры по **выявлению мошенничества**;
- Переоценка **соглашений и контрактов** с контрагентами, включая возможность «снятия риска» с контрагента, а также изменения или расторжения контракта.

2. Контрмеры, связанные с более строгим контролем за транзакциями контрагента

- Установка флага (метки) для просмотра транзакций, **превышающих заранее определенные пороги**. Они могут включать тип транзакции, сумму транзакции, валюту транзакции или профиль конечного бенефициара;
- В отношении всех помеченных флагом транзакций следует провести **дополнительную проверку**, например, ручной надзор с применением принципа четырех глаз и/или двустороннюю верификацию транзакции с контрагентом.

Приведенный выше перечень контрмер не является исчерпывающим, и учреждения могут использовать для управления риском и другие элементы контроля и инструменты.

Применение контрмер для контрагентов с более высоким уровнем риска

Для контрагентов с более высоким уровнем риска учреждения могут применять сочетание вышеуказанных контрмер. Как правило, учреждение применяет дополнительную проверку и отслеживает инструкции о производстве платежей, превышающих заранее определенное пороговое значение суммы или объема. Учреждение должно иметь возможность корректировать пороговые значения, а также обладать необходимыми инструментами и возможностями для обработки возросшего числа оповещений, а также дополнительными ресурсами для ручной обработки транзакции, включая необходимую актуальную контактную информацию контрагента.

Это состояние повышенного контроля не обязательно должно быть постоянным. Как только контрагенту удается перейти в категорию «низкого» риска, например, благодаря применению дополнительных контрмер, пороговые значения могут быть изменены или отменены.

Помимо решения о применении контрмер по уменьшению отрицательных последствий, каждое учреждение несет единоличную и исключительную ответственность за полное или частичное изменение, приостановление или прекращение отношений с контрагентом.

После того как процесс управления рисками в отношении кибербезопасности будет внедрен, структуре управления целесообразно проводить периодические проверки в отношении контрагента, чтобы оценить, изменился ли его профиль риска.

Голос клиента

Каким образом данные по аттестации в отношении кибербезопасности влияют на управление кибер-рисками, и какие органы управления участвуют в этом процессе?

«Еженедельные отчеты предоставляются нашему директору по управлению рисками наряду с предоставлением в другие отделы по управлению рисками. Мы отслеживаем количество предоставленных аттестаций по сравнению с количеством запросов, находящихся в процессе рассмотрения. Мы оцениваем риски всех предоставленных аттестаций, а затем применяем балльные оценки аттестаций к качественному профилю. Наши отделы по управлению рисками начали включать результаты оценки профилей в свои процессы».

Приложение A: Интеграция данных по аттестации, полученных от контрагентов SWIFT

Запущенная в мае 2016 года Программа обеспечения безопасности пользователей SWIFT (CSP) охватывает все пользовательские сегменты системы SWIFT с целью укрепления безопасности их локальной инфраструктуры в системе SWIFT.

Политика обеспечения безопасности пользователей SWIFT (CSCP) определяет процесс аттестации пользователей, а также соответствующие принципы, роли и обязанности. Система SWIFT также разработала Концепцию обеспечения безопасности пользователей SWIFT (CSCF), которая устанавливает исходный уровень обеспечения безопасности в виде применения элементов контроля, обязательных и рекомендуемых для всего сообщества пользователей.

Политика обеспечения безопасности пользователей SWIFT(CSCP) требует, чтобы пользователи самостоятельно проверяли наличие и применение **обязательных элементов контроля безопасности**, и призывает их также самостоятельно подтверждать наличие и применение рекомендуемых элементов контроля. Они подтверждают свой уровень соответствия, и их **аттестация** публикуется и управляется с помощью приложения KYC-Security Attestation (KYC-SA), предоставляемого SWIFT.

Ключевой функцией инструмента KYC-SA является возможность учреждений обмениваться данными по аттестации со своими контрагентами по взаимному согласию посредством **«запроса» и «предоставления» доступа**. Это позволяет учреждениям оценивать риск контрагента, а затем принимать решения в отношении риска контрагента на основе подтвержденных уровней соответствия. Данные по аттестации богаты информацией и являются уникальным источником данных о рисках в отношении кибербезопасности.

По мере того как учреждения начинают интегрировать данные аттестации CSP в свои концепции оценки риска контрагента, необходимо учитывать ряд факторов:

- соображения в отношении модели управления;
- соображения в отношении концепции управления рисками;
- дополнительные варианты контрмер по уменьшению отрицательных последствий.

Эти три области рассматриваются ниже в общем контексте инструмента KYC-SA.

Важно подчеркнуть, что пользователи, предоставляющие аттестацию, несут исключительную ответственность за ее достоверность, а SWIFT не проверяет точность информации, указанной в аттестациях пользователей. Программа обеспечения безопасности пользователей SWIFT (CSP) призвана обеспечить определенный уровень **стандартизации** и **прозрачности** предоставляемой информации по безопасности, который затем может применяться пользователями SWIFT.

В Приложении B содержатся ссылки на документы, посвященные Концепции обеспечения безопасности пользователей SWIFT (CSCF) и Политике обеспечения безопасности пользователей SWIFT (CSCP).

Приложение B также содержит ссылки на Рекомендации пользователю приложения KYC-SA, в которых приведены пошаговые инструкции о том, как запрашивать/предоставлять доступ к данным по аттестации и экспортировать данные по аттестации в виде файла Excel. Специалист по безопасности организации может экспортировать данные по аттестации каждого контрагента или соответствующих групп контрагентов. Однако эти рекомендации не ограничиваются описанием того, как организация должна использовать данные, то есть назначать управление, обрабатывать данные, оценивать риски и назначать контрмеры. Эти рекомендации изложены ниже.

Голос клиента

Каковы правила предоставления контрагентам доступа к вашим данным по аттестации? Является ли это общей ответственностью (например, отдела управления рисками, отдела нормативно-правового соответствия, юридического отдела и т.д.)?

«Процесс предоставления контрагентам доступа к нашим данным по аттестации требует участия нескольких отделов. Это позволяет обеспечить прозрачность предоставления доступа к нашим аттестациям. У нас есть внутренний процесс утверждения обработки данных. После внутреннего утверждения административный отдел предоставляет доступ посредством инструмента аттестации».

Соображения в отношении модели управления

Прежде чем принять решение о предоставлении данных по аттестации или направлять контрагенту запрос о предоставлении данных, необходимо определить общий процесс использования данных по аттестации контрагента. В частности, он должен определять, каким образом будет происходить передача данных и кто какую роль выполняет.

Хотя SWIFT предоставляет техническую платформу, модель управления учреждения также должна быть адаптирована таким образом, чтобы поддерживать оценку данных по аттестации в отношении безопасности контрагентов. Для «предоставления» или «запроса» доступа к данным по аттестации следует рассмотреть вопрос о том, какие соответствующие представители организации должны этим заниматься, и эти данные должны рассматриваться как дополнительный элемент в рамках существующей структуры управления рисками контрагента в организации.

Предоставление доступа контрагентам (или отказ в доступе)

Чтобы предоставить доступ по запросу контрагента, модель управления должна четко идентифицировать владельца бизнеса, управляющего процессом принятия решений «да» или «нет». Без четкого определения «лица, предоставляющего доступ» входящие запросы на аттестацию будут накапливаться и останутся без ответа.

Критерии принятия решения об удовлетворении входящих запросов, как правило, должны быть подписаны представителями комитета старших должностных лиц, например, Комитета по управлению рисками, или исполнительного руководства, например, директором по информационной безопасности, главным юрисконсультом или начальником отдела нормативно-правового соответствия.

Примерные критерии принятия решений в отношении предоставления доступа контрагентам, применяемые «лицом, предоставляющим доступ»

- Данные по аттестации будут переданы в банки, предоставляющие глобальные транзакционные услуги (Global Transaction Banks), независимо от их географического положения
- Данные по аттестации будут переданы контрагентам в том же местоположении с осуществлением надзора со стороны того же регулирующего органа
- Данные по аттестации будут переданы, как только мы сможем указать наш «Тип аттестации», подтвержденный внешней оценкой или аудитом.
- Данные аттестации будут переданы всем запрашивающим контрагентам, с которыми у нас есть активные отношения обмена сообщениями
- Данные аттестации будут переданы тем запрашивающим контрагентам, которые также передают свои данные по аттестации в наше учреждение
- Данные аттестации будут переданы всем запрашивающим контрагентам

Представители комитета старших должностных лиц или исполнительного руководства должны подписать критерии принятия решения. После этого руководство среднего звена сможет применять их к входящим запросам и предоставлять техническим операторам решения о предоставлении доступа или отказе в нем.

Исключения следует передавать на рассмотрение комитета старших должностных лиц или исполнительного руководства.

На оперативном уровне операторы (или «лица, предоставляющие доступ») должны регулярно (например, еженедельно) представлять руководству сводные данные по полученным запросам и предпринятым действиям.

Пример рабочего процесса по предоставлению доступа

1. Назначение оператора на роль «лица, предоставляющего доступ»
2. Оператор получает от контрагента запрос на предоставление доступа
3. Оператор рассматривает запрос на соответствие критериям утверждения и рекомендует положительный или отрицательный ответ
4. Руководство среднего звена рассматривает эту рекомендацию и либо дает разрешение на ее выполнение, либо предлагает альтернативное решение, либо передает вопрос на рассмотрение исполнительного руководства
5. Оператор «предоставляет» или «отклоняет» запрос контрагента В случаях отказа в доступе оператор должен иметь возможность указать причину отказа. Это может быть отсутствие отношений с контрагентом или неготовность предоставлять данные по аттестации в настоящее время.
6. Оператор должен регулярно (например, еженедельно) представлять сводные данные по статусам запросов и предпринятым действиям

Инструмент аттестации также предоставляет возможность создания «белого списка» контрагентов BIC, которые соответствуют критериям, определенным исполнительным руководством. Это позволит по запросу автоматически предоставлять доступ таким контрагентам, избегая необходимости ручного анализа и утверждения. Эта функция известна как «Автопредоставление».

Запрашивание доступа у контрагентов

Представители комитета старших должностных лиц или исполнительного руководства должны подписать критерии предоставления доступа контрагентам. Критерии запроса данных по аттестации у контрагента должны быть определены на аналогичном уровне руководства.

Примерные критерии принятия решения, используемые «лицом, запрашивающим доступ» для направления запроса на доступа к данным контрагента

- Мы будем запрашивать данные по аттестации у всех наших контрагентов
- Мы будем запрашивать данные по аттестации только у контрагентов, с которыми мы взаимодействуем нерегулярно
- Мы будем запрашивать данные по аттестации только у контрагентов, которые расположены в зоне высокого риска
- Мы будем запрашивать данные по аттестации только у контрагентов с высоким уровнем риска

Как только критерии принятия решений будут определены исполнительным руководством, оператор («лицо, запрашивающее доступ») будет направлять запросы на аттестацию в инструменте аттестации.

Статусы запросов на доступ к данным по аттестации контрагентов должны регулярно (например, еженедельно) сообщаться руководству — аналогично статусам по предоставлению доступа контрагентам.

Пример рабочего процесса по направлению запроса на доступ

1. Назначение оператора на роль «лица, запрашивающего доступ»
2. Исполнительное руководство определяет критерии принятия решения для направления запроса на доступ к данным по аттестации контрагента
3. Оператор направляет запрос контрагенту через инструмент аттестации
4. Контрагент «предоставляет» или «отклоняет» запрос на доступ В случаях, когда запрос был отклонен, исполнительному руководству следует рассмотреть вопрос о дальнейшем взаимодействии с контрагентом и повторно запросить доступ после устранения причины отказа.
5. Оператор должен регулярно (например, еженедельно) представлять сводные данные по статусам запросов и предпринятым действиям

Голос клиента

Подтолкнула ли вас какая-либо информация, полученная в результате получения доступа к данным по аттестации контрагентов, к принятию важного решения в отношении кибербезопасности? Если да, уточните, пожалуйста, какая именно?

«После того, как нам предоставляют доступ к данным по аттестации контрагента, мы просматриваем ответы на эти элементы управления. Хотя мы еще не принимали решения в отношении кибербезопасности на основе данных по аттестации контрагентов, ответы контрагентов активизировали наши внутренние процессы в сфере кибербезопасности».

Соображения в отношении концепции управления рисками

Организации, которым был предоставлен доступ к данным по аттестации контрагента, могут использовать инструмент приложения для «использования» данных. Эти данные по аттестации, включающие уровни соответствия по каждому элементу контроля, следует интегрировать в систему принятия решений, основанную на оценке рисков, чтобы минимизировать риск, связанный с контрагентом.

Учреждения, желающие интегрировать данные по аттестации в отношении кибербезопасности в свой существующий процесс управления рисками, могут использовать коэффициенты взвешенной значимости и баллы на основе этой информации.

Пример подхода к использованию коэффициентов взвешенной значимости и баллов

- Если контрагент не предоставил аттестацию, ему должен быть поставлен определенный балл
- Если контрагент не ответил на запросы на доступ в KYC-SA, ему должен быть поставлен определенный балл
- Следует присудить баллы уровням соответствия по каждому элементу контроля в рамках Концепции обеспечения безопасности пользователей SWIFT (CSCF): например, соответствие рекомендациям, соответствие альтернативными способами, несоответствие или соответствие в будущем к определенной дате
- Каждому конкретному элементу контроля, обязательному или рекомендуемому, может быть присвоен какой-либо коэффициент взвешенной значимости
- Другим аттестационным переменным может быть присвоен определенный коэффициент взвешенной значимости, например:
  - **Тип инфраструктуры**
  - **Компоненты инфраструктуры** — использует ли контрагент сертифицированный интерфейс?
  - **Поставщик услуг** — подключается ли контрагент через поставщика услуг и каков статус сертификации или соответствия этого поставщика?
  - **Тип оценки** — привлекал ли контрагент внутренние или внешние третьи стороны для получения консультаций или его аттестация была подтверждена внутренней или внешней независимой оценкой? Смотрите ниже.

Присуждение значимых коэффициентов взвешенной значимости и баллов — это процесс, для которого учреждения должны обеспечивать сотрудничество между внутренними заинтересованными сторонами, такими как отдел информационной безопасности, операционный отдел, отдел технологий, отдел управления рисками, отдел нормативно-правового соответствия, отдел по поддержке бизнеса и юридический отдел.

Интерпретация «типа оценки»

Это поле в самоаттестации отражает степень, в которой контрагент пользовался услугами независимых рецензентов для подтверждения уровня своего соответствия, указанного в аттестации

– **Сторонняя независимая оценка (может включать аудит, проводимый внешним аудитором)** — учреждение подтвердило соответствие контролю посредством использования услуг независимого внешнего оценщика. Название компании-аудитора должно быть объявлено учреждением, предоставляющим аттестацию. – **Внутренняя независимая оценка (может включать внутренний аудит)** — учреждение подтвердило соответствие контролю посредством использования услуг внутреннего оценщика.	Обеспечивает более высокую степень обоснованной уверенности в том, что статус соответствия, присвоенный каждому элементу контроля, был подтвержден независимо. Предполагает более высокий уровень доверия к контрагентам, которые могут предоставить этот уровень подтверждения. Позволяет провести проверку данных компании-внешнего оценщика.
– **Консультативное рассмотрение внешней фирмой** — при оценке соответствия организация привлекла третье лицо для оказания консультативных услуг. Название сторонней компании должно быть объявлено учреждением, предоставляющим аттестацию. – **Консультативное рассмотрение внутренними независимыми группами** — при оценке соответствия организация привлекла независимую внутреннюю сторону для оказания консультативных услуг.	Обеспечивает некоторую степень уверенности в независимом подтверждении указанного статуса элемента контроля. Консультативные оценки не выполняются в рамках фиксированных, заранее определенных процессов. Степень уверенности может быть выше, если будет подготовлен и предоставлен полный отчет об оценке. Может быть дополнен целевой оценкой или выборочной проверкой.
– **Самоаттестация** — учреждение самостоятельно оценило свое соответствие, например, посредством подписания аттестации директором по информационной безопасности, КИО или другим исполнительным руководством.	Обеспечивает минимальную степень уверенности в том, что контрагент тщательно оценил свое соответствие элементам контроля в рамках Концепции обеспечения безопасности пользователей SWIFT.

Дополнительные меры по снижению рисков

Помимо общих контрмер, изложенных в Разделе 4, процесс рассмотрения может быть расширен и включать ряд дополнительных вариантов, специфичных для использования системы SWIFT, как указано ниже.

Запрос соответствия рекомендуемым элементам контроля

Помимо существующего обязательства по предоставлению самоаттестации в отношении набора обязательных элементов контроля учреждения могут запросить, чтобы некоторые контрагенты также самостоятельно подтвердили применение некоторых или всех рекомендуемых элементов контроля.

Применение контрагентом мер по выявлению мошенничества

Пользователи SWIFT могут запросить, чтобы некоторые контрагенты внедрили механизмы выявления мошенничества, обнаруживающие аномальные или выпадающие показатели, отличающие от нормальной модели поведения. В настоящее время в Концепции обеспечения безопасности пользователей SWIFT версии 2019 года это определяется как Консультативный контроль.

Например: Ежедневные отчеты по валидации SWIFT (DVR)

В рамках Программы обеспечения безопасности пользователей (CSP), система SWIFT расширила свой портфель соответствия требованиям по борьбе с финансовыми преступлениями, внедрив инструмент обнаружения шаблонов транзакций. Он был разработан с целью снижения рисков, связанных с мошенничеством в сфере платежей.

Ежедневные отчеты по валидации (DVR) позволяют учреждениям легко проверять активность платежных транзакций, выявлять потенциальные риски и быстро реагировать на случаи мошенничества.

DVR предоставляет информацию о платежных операциях за предыдущий день. Общая сумма и объем транзакций за каждый день сравниваются с ежедневными средними значениями и объемами транзакций пользователя за предыдущие 24 месяца, что позволяет быстро выявлять существенные изменения в деятельности.

Охвачены две ключевые области:

- Отчеты об активности позволяют пользователям видеть их агрегированную ежедневную активность. Агрегированная ежедневная активность предоставляется с указанием типа сообщения, валюты, страны и контрагента. Предоставляются ежедневные общие суммы и объем транзакций, а также подробная информация о самых крупных транзакциях.
- Отчет о рисках предназначен для выявления больших или необычных потоков сообщений, которые могут указывать на риски мошенничества. Он помогает пользователям выбирать самые крупные отдельные транзакции и самые крупные потоки агрегированных транзакций своих контрагентов в виде входящих и исходящих платежей. Сравнения с предыдущими среднесуточными значениями и объемами позволяют пользователям оценить изменения в активности. Отчет о рисках также выявляет новые комбинации прямых и косвенных контрагентов по транзакциям в течение этого дня.

Информация агрегируется для следующих ключевых типов сообщений SWIFT: MT 103, MT 202, MT 202COV, MT 205 и MT 205COV.
Ежедневные отчеты по валидации SWIFT (DVR) были внедрены в 2016 году.

Например: Сервис контроля платежей SWIFT (PCS)

Сервис контроля платежей (PCS) помогает пользователям SWIFT незамедлительно выявлять аномальную активность. Сервис PCS в режиме реального времени обнаруживает платежи, которые не соответствуют политике контрагента, являются нехарактерными и указывают на риск мошенничества. Он выполняется внешне, то есть вне помещений пользователя. Это подразумевает, что даже если нарушена безопасность учреждения, данные остаются достоверными.

Сервис PCS работает в реальном времени в одном из двух режимов, используя правила политики, определенные подписчиком:

- копирование сообщения и оповещение; или
- удержание сообщения и оповещение.

В сущности, сервис PCS позволяет пользователям настраивать правила политики по ряду параметров:

- бизнес-календари, нерабочие дни и обычное рабочее время;
- белый/черный списки валют, лимиты на единовременный и агрегированный платеж;
- белый/черный списки стран, лимиты на единовременный и агрегированный платеж;
- пороговые значения для комбинации стран, валют, отдельной организации или их группы;
- новые учреждения: определяются платежи с новыми участниками или цепочками, основываясь на исторических потоках сообщений;
- подозрительные счета: сверка номеров счетов конечных клиентов с черным списком учреждения, где указаны номеров счетов с высоким уровнем риска.

Сервис PCS был запущен в октябре 2018 года.

Обратите внимание, что до того как учреждение внедрит элементы контроля с целью выявления мошенничества со стороны получателя или до того как учреждение запросит контрагента применить элементы контроля с целью выявления мошенничества со стороны отправителя, необходимо ознакомиться с Условиями и положениями и другими юридическими аспектами.

Улучшение и укрепление взаимодействия с приложением для управления взаимоотношениями с контрагентами Relationship Management Application (RMA)

Отношения, установленные несколько лет назад, могли со временем измениться и перестать соответствовать бизнес-моделям сегодняшнего дня. Помимо контроля над тем, кто может отправлять сообщения с помощью Приложения для управления взаимоотношениями с контрагентами Relationship Management Application (RMA), пользователи системы SWIFT могут ограничивать типы сообщений с RMA+. Например, пользователь может согласиться получать казначейские или торговые сообщения, но не платежные сообщения.

Например: SWIFT RMA и RMA Plus

Приложение для управления взаимоотношениями с контрагентами Relationship Management Application (RMA) — это процесс обмена ключами и авторизации между двумя финансовыми учреждениями, позволяющий им определить, какие контрагенты могут отправлять им сообщения FIN. Любой нежелательный трафик блокируется на уровне отправителя, что снижает операционные риски, связанные с обработкой нежелательных сообщений.

RMA Plus — усовершенствованная версия приложения RMA, позволяющая учреждениям указывать, какие типы сообщений они хотят отправлять и получать от каждого из своих контрагентов. Например, учреждение может решить получать аккредитивы только от определенного корреспондента.

Для получения сообщений от своих контрагентов учреждениям необходимо предоставить авторизацию в приложениях RMA или RMA Plus этим контрагентам, а функциональные возможности RMA встроены в интерфейсы SWIFT Alliance Access и Alliance Entry.

Многие учреждения со временем установили отношения со многими контрагентами в приложении RMA. Однако список авторизаций RMA не всегда обновляется при изменении или прекращении деловых отношений. Поэтому у учреждений может быть большое количество неактивных RMA — они могут даже не знать о них.

Рационализируя и отменяя неактивные отношения в RMA, учреждения минимизируют время и затраты, связанные с такой деятельностью, а также снижают риски.

Учреждения могут самостоятельно решить эту задачу по рационализации. В качестве альтернативы SWIFT предлагает услугу «очистки» авторизаций RMA и RMA Plus.

Приложение для управления взаимоотношениями с контрагентами Relationship Management Application (RMA) было запущено в 2009 году.

Приложение B: Глоссарий

Термин	Акроним	Описание
Программа обеспечения безопасности пользователей SWIFT	CSP	**Нажмите здесь для получения дополнительной информации**
Концепция обеспечения безопасности пользователей SWIFT	CSCF	**Нажмите здесь для получения дополнительной информации**
Политика обеспечения безопасности пользователей SWIFT	CSCP	**Нажмите здесь для получения дополнительной информации**
Знай своего клиента — Аттестация по безопасности (приложение)	KYC-SA	Исходный уровень: **Нажмите здесь для получения дополнительной информации** Руководство пользователя: **Нажмите здесь для получения дополнительной информации**
Приложение для управления взаимоотношениями с контрагентами Relationship Management Application	RMA	**Нажмите здесь для получения дополнительной информации**
Ежедневные отчеты по валидации	DVR	**Нажмите здесь для получения дополнительной информации**
Сервис контроля платежей	PCS	**Нажмите здесь для получения дополнительной информации**
Поставщик общей инфраструктуры	SIP	**Нажмите здесь для получения дополнительной информации**
Идентификационный код предприятия	BIC	**Нажмите здесь для получения дополнительной информации**
Директор по информационной безопасности	CISO	Общее название должности, используемое для обозначения самого высокопоставленного руководителя, ответственного за информационную безопасность компании.

О SWIFT

SWIFT является глобальным кооперативным сообществом и ведущим в мире поставщиком услуг безопасного обмена финансовыми сообщениями. Мы предоставляем нашему сообществу стандарты и платформу для обмена сообщениями, а также предлагаем продукты и услуги для облегчения доступа и интеграции, идентификации, анализа и соблюдения стандартов безопасности.

Наша платформа обмена сообщениями, продукты и услуги объединяют более 11 000 банковских организаций, участников рынка ценных бумаг, рыночных инфраструктур и корпоративных клиентов в более чем 200 странах и территориях, позволяя им безопасно общаться и обмениваться стандартизированными финансовыми сообщениями.

Будучи надежным поставщиком услуг, SWIFT постоянно совершенствует свой подход в работе, поддерживает коммерцию во всем мире и повышает эффективность операционных процессов с целью снижения затрат и рисков.

Международное руководство SWIFT осуществляется из штаб-квартиры в Бельгии и поддерживает принципы глобального сотрудничества. Международная сеть офисов SWIFT обеспечивает присутствие во всех крупных финансовых центрах мира.

Для получения дополнительной информации посетите сайт www.swift.com, обратитесь к вашему менеджеру по работе с клиентами или отправьте нам сообщение по адресу электронной почты weareswift@swift.com.

57386 – январь 2019 г.